

*«Информационная безопасность: современные технологии»
Ижевск, 21 мая 2009*

Информационная безопасность в Удмуртской Республике: решения компании «Ижинформпроект»

Майшев Вадим Владимирович

*Заместитель генерального директора по
безопасности*



НПП «Ижинформпроект»

- ♦ автоматизация бизнес-процессов
- ♦ услуги телематических служб и передачи данных
- ♦ услуги по контролю движения транспортных средств с помощью систем глобального позиционирования
- ♦ поставка, установка, настройка и сопровождение средств и систем защиты информации
- ♦ услуги специализированного оператора связи по обеспечению представления отчетности в контролирующие органы
- ♦ услуги по организации защищенного электронного документооборота и защищенного межсетевому взаимодействию
- ♦ услуги Удостоверяющего центра InfoTrust
- ♦ консультационные услуги в области информационной безопасности



Лицензии

Управление ФСБ России по Удмуртской Республике

- ♦ на право распространения шифровальных (криптографических) средств № 01 от 22.08.2008
- ♦ на право технического обслуживания шифровальных (криптографических) средств № 02 от 22.08.2008
- ♦ на право предоставления услуг в области шифрования информации № 03 от 22.08.2008



Россвязьохранкультура

- ♦ на право предоставления услуг связи по передаче данных № 59491 от 18.08.2008
- ♦ на право предоставления телематических услуг связи № 59492 от 18.08.2008



Информационная безопасность

- ◆ поставка, установка, настройка и техническая поддержка и сопровождение средств защиты информации
- ◆ консультационные услуги в области информационной безопасности
- ◆ Удостоверяющий центр InfoTrust
- ◆ защищенный электронный документооборот
- ◆ защищенное межсетевое взаимодействие



Средства защиты информации

- ◆ **Криптографическое ядро** (КриптоПро CSP, Домен-К, Верба, КРИПТОН/Crypton, Дионис, LirSSL)
- ◆ **Шифратор дисков** (Secret Disk, Crypton Disk, ViPNet [Safe Disk])
- ◆ **Файловый криптоменеджер** (КриптоАРМ, Верба-Клиент, DiSignCA, Блокхост-ЭЦП)
- ◆ **Электронные ключи и идентификаторы** (eToken PRO, ruToken, ШИПКА)
- ◆ **Электронный замок** (Соболь, Аккорд-АМДЗ, КРИПТОН-ЗАМОК)
- ◆ **Программно-аппаратный комплекс СЗИ НСД** (Secret Net, Security Studio, Аккорд-NT/2000, DALLAS LOCK, Блокхост, Панцирь, Страж)
- ◆ **Программно-аппаратный комплекс СЗИ НСД для работы в локальной сети** (Secret Net, Security Studio, DALLAS LOCK, Панцирь, АккордСеть)



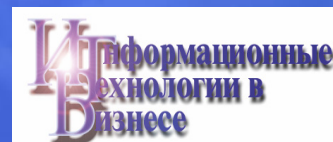
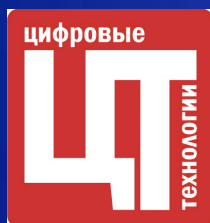
Средства защиты информации

- ◆ **Межсетевые экраны** («Континент», ViPNet [Office Firewall], ДИОНИС, «NetScreen»)
- ◆ **Персональные сетевые экраны** («Континент», ViPNet [Personal Firewall], «Блокпост-экран»)
- ◆ **Криптомаршрутизаторы /VPN** (АПКШ «Континент», ViPNet [CUSTOM], ДИОНИС, КРИПТОН-IP)
- ◆ **VPN-агенты** («Континент-АП», ViPNet [Клиент], DiSec, Crypton IP Mobile)
- ◆ **Антивирусные средства** (Kaspersky, Dr.WEB)
- ◆ **Средства управления ИБ** (КУБ)
- ◆ **Специальное ПО для анализа рисков** (Digital Security Office)



Партнеры

НПП «Ижинформпроект»



Консультационные услуги

- ◆ Проведение обследования объекта, применяемых деловых процедур и информационно-телекоммуникационной системы (как объекта защиты), анализ ее структуры, функций и особенностей, используемых технологий автоматизированной обработки и передачи информации, анализ выполняемых бизнес-процессов, анализ нормативной и технической документации
- ◆ Выявление значимых угроз, разработка политики безопасности и рекомендаций по защите конфиденциальной информации и персональных данных
- ◆ Разработка необходимых организационно-распорядительных и нормативных документов
- ◆ Поставка, установка, настройка и техническое сопровождение программно-аппаратных средств защиты информации, в т.ч. криптографических
- ◆ Комплекс услуг по внедрению, развитию и сопровождению различных видов защищенного (в т.ч. юридически значимого) электронного документооборота и межсетевого взаимодействия (VPN и удаленный доступ)
- ◆ Комплекс услуг специализированного оператора связи, удостоверяющего центра, а также внешних служб технической и криптографической защиты информации (АУТСОРСИНГ)



Защищенные IT-сервисы

- ◆ Корпоративная защищенная информационно-телекоммуникационная система КriptoСвязь:
 - ОТЧЕТНОСТЬ через ИНТЕРНЕТ
 - Защищенный Электронный Документооборот
 - Virtual Private Network
 - ...
- ◆ КriptoСвязь = ИБ(Криптография/УЦ/VPN) + телекоммуникации



Эффективность электронного документооборота

- ◆ Повышение производительности труда сотрудников, связанных с подготовкой, формированием и использованием документов
- ◆ Сокращение трудоемкости обработки данных
- ◆ Сокращение количества ошибок, связанных с переносом данных из бумажных документов в информационные системы
- ◆ Уменьшение затрат на канцелярские принадлежности, автотранспорт
- ◆ Достижение необходимого уровня исполнительской дисциплины
- ◆ Повышение качества и оперативности принятия управленческих решений
- ◆ Организация доступа к знаниям, накопленным в виде массы документов
- ◆ Повышение эффективности и эффективности бизнес-процессов и государственного и муниципального управления



Электронный документооборот?



- ◆ «Электронный документооборот должен стать реальностью» (Д.Медведев, 17.07.2008)
- ◆ «...Внутренний документооборот до сих пор ведется на бумаге, компьютеры используются как пишущие машинки. Мы пятый год переводим нашу работу в электронный вид. На рассылку документов по ведомствам уходят тонны бумаги. Так никто не делает, а мы очень богатые и леса у нас много» (Д.Медведев, 12.02.2009)



Бумажный vs Электронный



- ◆ Удобство формирования!
- ◆ Как хранить?
- ◆ Как транспортировать?



- ◆ Переходим на электронный!!!
- ◆ А БЕЗОПАСЕН ли он ???

Защищенный электронный документооборот

- ◆ Конфиденциальность
- ◆ Целостность
- ◆ Достоверность
- ◆ Аутентичность
- ◆ Неотказуемость
- ◆ Юридическая значимость



Электронная цифровая подпись

ЭЦП - метод защиты информации, обеспечивающий возможность контроля целостности и подтверждения подлинности ЭД. При этом ЭЦП должна обеспечивать выполнение следующих функций:

- ◆ подтверждать, что подписывающее лицо не случайно подписало электронный документ;
- ◆ подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ;
- ◆ зависеть от содержания подписываемого документа и времени его подписания;
- ◆ подписывающее лицо не должно иметь возможности в последствии отказаться от факта передачи документа.

Электронная цифровая подпись

В соответствии с Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»:

ЭЦП - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Криптографическая защита информации

Криптографическое преобразование - это преобразование информации, основанное на некотором математическом алгоритме, зависящем от изменяемого параметра (ключ), и обладающее свойством невозможности восстановления исходной информации без знания действующего ключа.

К основным криптографическим методам защиты относятся:

- **шифрование** информации (зашифрование и расшифрование),
- формирование и проверка **электронной цифровой подписи** ЭД.

◆ Достоинство - высокая гарантированная стойкость защиты.

◆ Недостатки:

- значительные затраты ресурсов на выполнение преобразований;
- сложности управления криптографическими ключами;
- высокие требования к сохранности секретных ключей и защите от подмены.



Функции УЦ по обеспечению безопасности взаимодействия

- ◆ регистрирует ключи ЭЦП;
- ◆ создает по обращению пользователей закрытые и открытые ключи ЭЦП;
- ◆ приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ◆ ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;
- ◆ выдает сертификаты ключей подписей на бумажных носителях и в виде электронных документов с информацией об их действительности;
- ◆ проводит, по обращениям пользователей, подтверждение подлинности (действительности) подписи в ЭД в отношении зарегистрированных им ЭЦП.



Создание системы защищенного электронного документооборота

- ◆ Лицензии на деятельность в области криптографической защиты информации
- ◆ Партнерские отношения с производителями средств защиты информации
- ◆ Удостоверяющий центр (персонал, технологические аспекты, организационные документы, технические средства, средства защиты информации)
- ◆ Система защищенного электронного документооборота (организационные документы, технические и технологические аспекты)



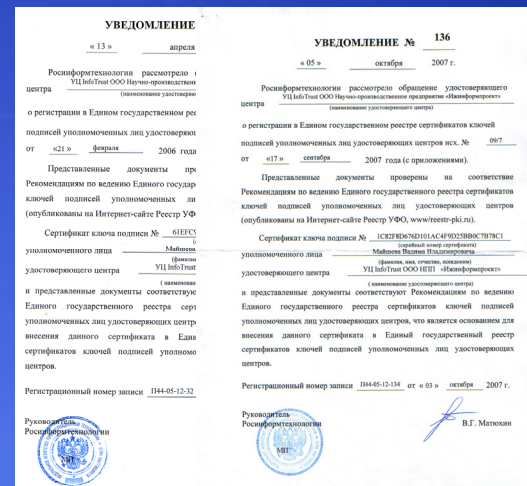
Удостоверяющий центр InfoTrust

- ◆ Начал функционировать в 2005 году
- ◆ Основание деятельности – лицензии ФСБ России в области криптографической защиты информации
- ◆ Цель – управление криптографическими ключами пользователей защищенных сервисов
- ◆ Аттестован по требованиям безопасности для обработки конфиденциальной информации



Соответствие законодательству

- ◆ Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров
www.reestr-pki.ru
- ◆ Российские криптографические алгоритмы:
ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94,
ГОСТ 28147-89
- ◆ Сертифицированные средства криптографической защиты информации «КриптоПро CSP»
- ◆ Сертифицированный программно-аппаратный комплекс «Удостоверяющий Центр «КриптоПро УЦ»



Соответствие законодательству

- ◆ Указание в сертификате сведений об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическую силу

- ◆ Регистрация в мировом «дереве» идентификаторов объектов



{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1)
IzhInformProject(23133)}

<http://www.iana.org/assignments/enterprise-numbers>

- ◆ Регистрация в российском «дереве» идентификаторов объектов

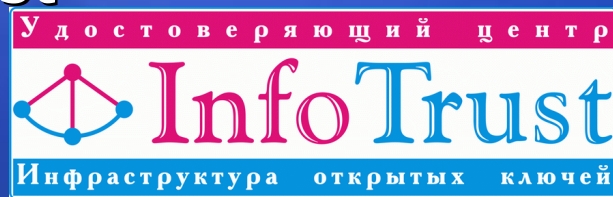


{iso(1) member-body(2) ru(643) REG1(1) IzhInformProject(10)}
{iso(1) member-body(2) ru(643) REG3(3) IzhInformProject(34)}

<http://www.ctel.msk.ru/x500/OIDS/inform.htm>

Регламентация деятельности УЦ

- ◆ Регламент Удостоверяющего центра InfoTrust (Certification Practice Statement — CPS)
- ◆ Правила применения сертификатов Удостоверяющего центра InfoTrust (Certificates Policy — CP)
- ◆ Справочник по Инфраструктуре открытых ключей Удостоверяющего центра InfoTrust (PKI Disclosure Statement — PDS)
- ◆ Перечень объектных идентификаторов ООО НПП «Ижинформпроект» (OID index)
- ◆ Памятка пользователю Удостоверяющего центра InfoTrust



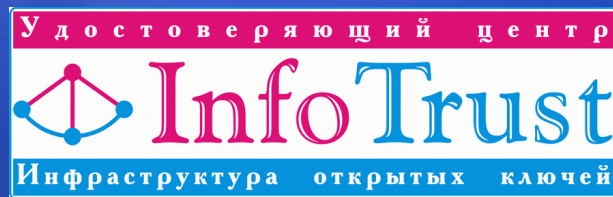
Регламент Удостоверяющего центра

- ◆ Содержит порядок выполнения процедур:
 - регистрации пользователей,
 - генерации ключевых документов,
 - формирования запросов на сертификат,
 - изготовления сертификата,
 - отзыва сертификата,
 - приостановления/возобновления действия сертификата.
- ◆ Условие получения услуг Удостоверяющего центра –присоединение к Регламенту УЦ (договор присоединения) в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации



Регламент Удостоверяющего центра

- ◆ Содержит шаблоны документов, оформляемых при взаимодействии пользователя и Удостоверяющего центра при выполнении операций по управлению ключами и сертификатами:
 - Подписной лист к Регламенту;
 - Заявление о регистрации пользователя УЦ;
 - Заявление об изготовлении сертификата;
 - Заявления об аннулировании/ приостановлении/ возобновлении действия сертификата.



Правила применения сертификатов

- ◆ Содержит требования к регистрации пользователей;
- ◆ Содержит требования по информационной безопасности;
- ◆ Регламентирует применение сертификата для разрешенных приложений и систем с установленными требованиями безопасности:
 - защита соединений в Интернете с использованием протокола TLS/SSL — проверка подлинности сервера и клиента;
 - защищенная электронная почта с использованием стандарта S/MIME (электронная цифровая подпись для аутентификации отправителя и гарантии подлинности и целостности сообщения и шифрование данных);
 - компоненты с электронной цифровой подписью (электронная цифровая подпись электронных документов и кода программ);
 - штампы времени и службы актуального статуса сертификатов



«КриптоСвязь»

{ОТЧЕТНОСТЬ через ИНТЕРНЕТ}

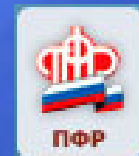
◆ Технологическое лидерство

- РКИ/СКЗИ+УЦ (КРИПТО-ПРО, Москва)
- Технология «Контур-Экстерн» (СБ Контур, Екатеринбург)
- ~60 % в России, ~80 % в Удмуртии



◆ Широчайший спектр сервисов

- Отчетность в ФНС России с 2003
- Отчетность в ПФР с 2007
- Отчетность в Росстат с 2007
- Отчетность в Ростехнадзор с 2009
- Отчетность в Минторгбыт Удмуртии с 2009
- ...



«КриптоСвязь»

{Защищенный Электронный Документооборот}

- ◆ Обеспечивает конфиденциальность, целостность, достоверность, аутентичность, неотказуемость и юридическую значимость электронных документов
- ◆ Обработка конфиденциальной информации (персональные данные, служебная, коммерческая, профессиональная, банковская тайна и т.п.)
- ◆ Электронная цифровая подпись (+ шифрование) электронных документов, представленных в виде файлов, электронная цифровая подпись и шифрование сообщений электронной почты по протоколу S/MIME и защита Интернет-соединений по протоколу TLS с применением российских ГОСТов
- ◆ Сертифицированные средства криптографической защиты информации
- ◆ Соответствие закону «Об электронной цифровой подписи»
- ◆ Функционирует с 2006 года

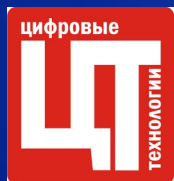


Регламентация системы «КриптоСвязь» {Защищенный Электронный Документооборот}

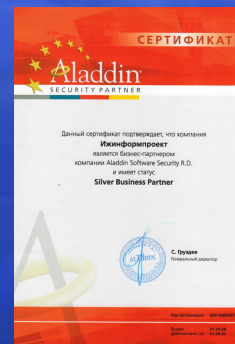
- ◆ Регламент защищенного электронного документооборота в системе «КриптоСвязь»
- ◆ Условия оказания услуг в системе
- ◆ Технические условия подключения автоматизированного рабочего места
- ◆ Положение о порядке использования средств криптографической защиты информации и ключевой информации к ним
- ◆ Требования по обеспечению безопасности автоматизированного рабочего места
- ◆ Положение по разрешению споров, связанных с подлинностью электронных документов
- ◆ Памятка пользователю средств криптографической защиты информации



Состав АРМ-ЗЭД

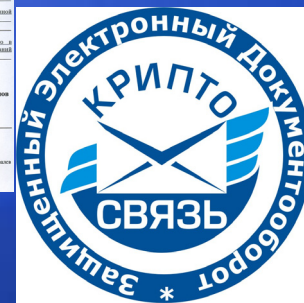


- ◆ сертифицированное средство криптографической защиты информации «КриптоПро CSP»
- ◆ Криптографический файловый менеджер «КриптоАРМ» Стандарт/СтандартPRO
- ◆ Клиент защищенной электронной почты (Outlook Express, MicroSoft Outlook – с поддержкой S/MIME) и защищенный Интернет-браузер (Internet Explorer – с поддержкой TLS)
- ◆ устройство защищенного хранения криптографических ключей (eToken PRO (Java) или РУТОКЕН)
- ◆ Средство защиты информации от несанкционированного доступа - опционально (Secret Disk, Соболь, Аккорд)
- ◆ Сертификат ключа подписи Удостоверяющий центр InfoTrust



Сертификаты соответствия на компоненты

- ◆ КриптоПро CSP версия 2.0 — ФCB России № СФ/114-1001
- ◆ КриптоПро CSP версия 3.0 — ФCB России № СФ/144-1174
- ◆ Заключение о корректности встраивания СКЗИ КриптоПро CSP в ПО «КриптоАРМ»
- ◆ eToken — ФСТЭК России № 925/5
- ◆ «eToken — «КриптоПро» CSP» — сертификат совместимости от 01.09.2008
- ◆ RUOKEN — ФCB России №СФ/124-0999, ФСТЭК России № 1461
- ◆ Secret Disk — ФСТЭК России № 1742
- ◆ Собыль — ФСТЭК России № 907, 1574, ФCB России № СФ/027-0887
- ◆ Аккорд — ФСТЭК России № 246/7, ФCB России № СФ/127-1082



Структура АРМ-ЗЭД



Комплекты для АРМ-ЗЭД

комплект	Компонент	СКЗИ КriptoПро CSP	КriptoАРМ	eToken PRO*	РУТОКЕН*	Secret Disk*	СКП «ИНФРА»	СКП «УЛЬТРА»	СКП «ТРАСТ»
СТАНДАРТ		☑	☑	☑				☑	
СТАНДАРТ-РУ		☑	☑		☑		☑		
ПРОФИ		☑	☑	☑		☑		☑	
ДУЭТ		☑	☑	☑					☑

ИНФРА — защищенная электронная почта (S/MIME)

УЛЬТРА — аутентификация клиента и защищенная электронная почта (TLS + S/MIME)

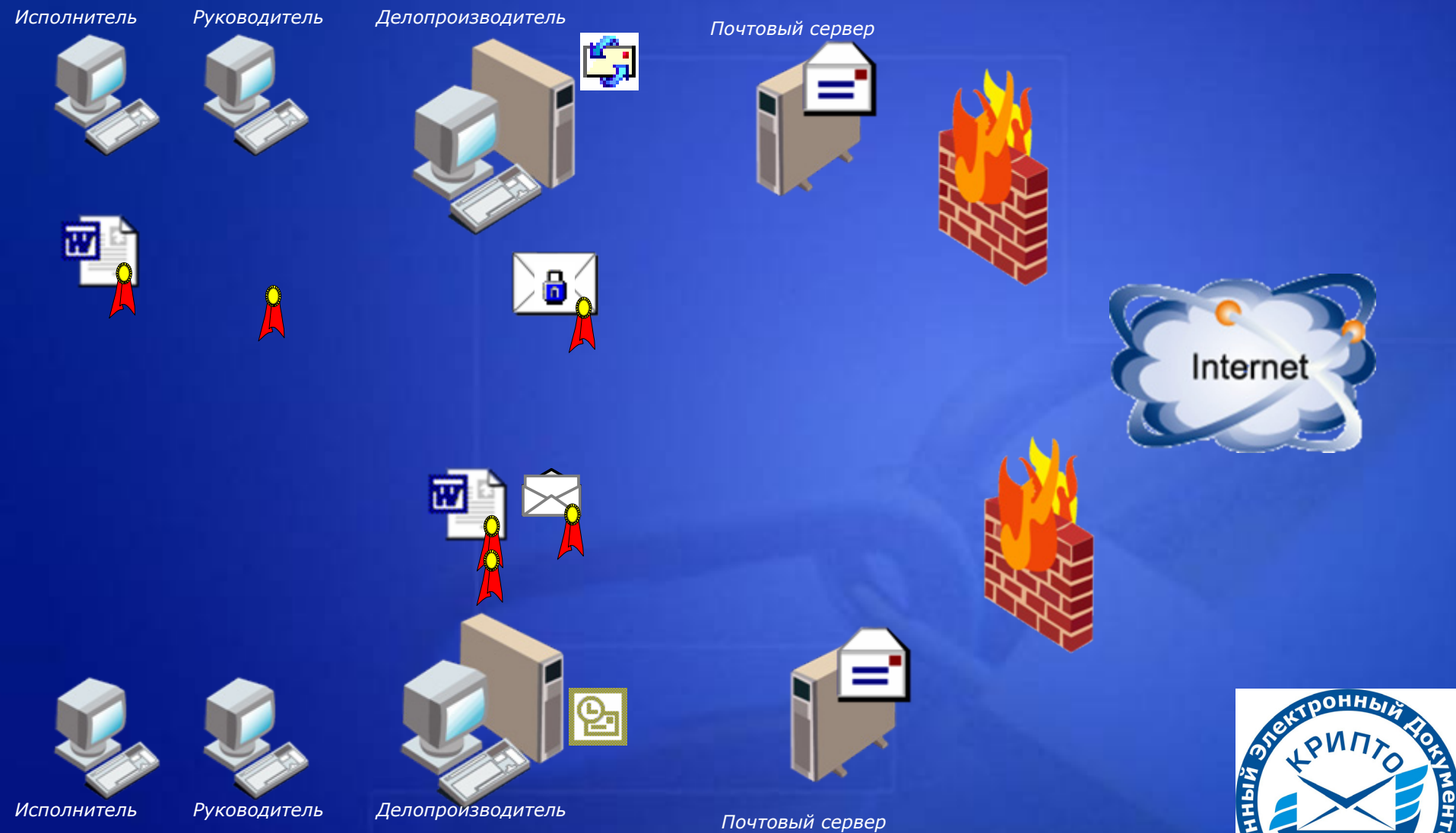
ТРАСТ — универсальный сертификат (+ *Отчетность в контролирующие органы*)

ДУЭТ — «КриптоСвязь»{Защищенный Электронный Документооборот}
+ «КриптоСвязь»{ОТЧЕТНОСТЬ через ИНТЕРНЕТ}

* — опционально поставляются компоненты с сертификатами соответствия
ФСБ России и ФСТЭК России



Типовая схема движения документов



Комплекс услуг

◆ Подключение, поставка и внедрение:

- подключение и поставка средств защиты информации
- установка и настройка АРМ-ЗЭД, настройка параметров защищенного электронного документооборота
- обучение пользователя

◆ Техническая поддержка и сопровождение:

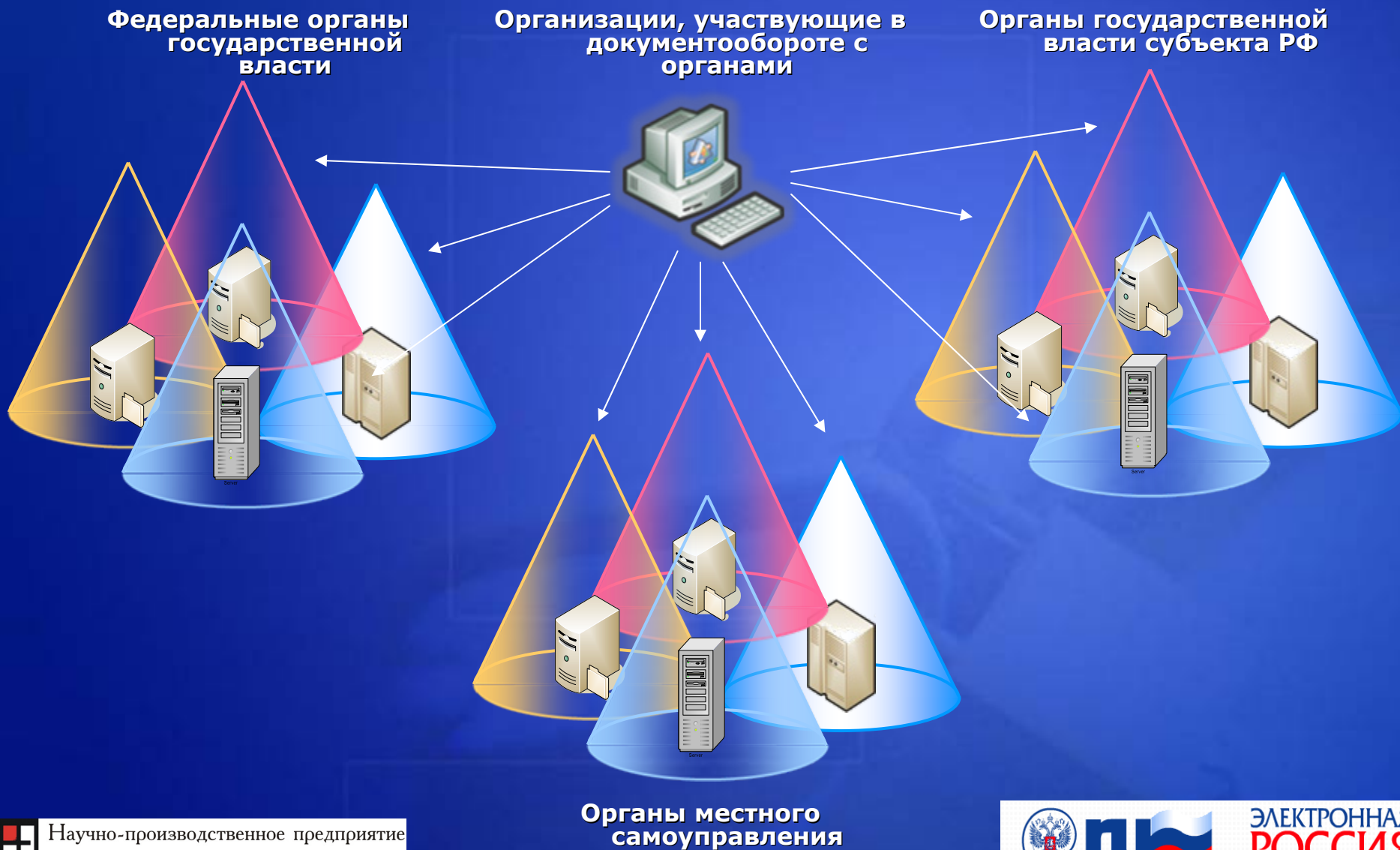
- сопровождение регламента защищенного электронного документооборота
- техническая поддержка пользователя
- работы по техническому сопровождению АРМ-ЗЭД

◆ Консультационные услуги:

- Разработка организационно-распорядительных документов и специальных регламентов



Использование ЭЦП в сфере государственного управления



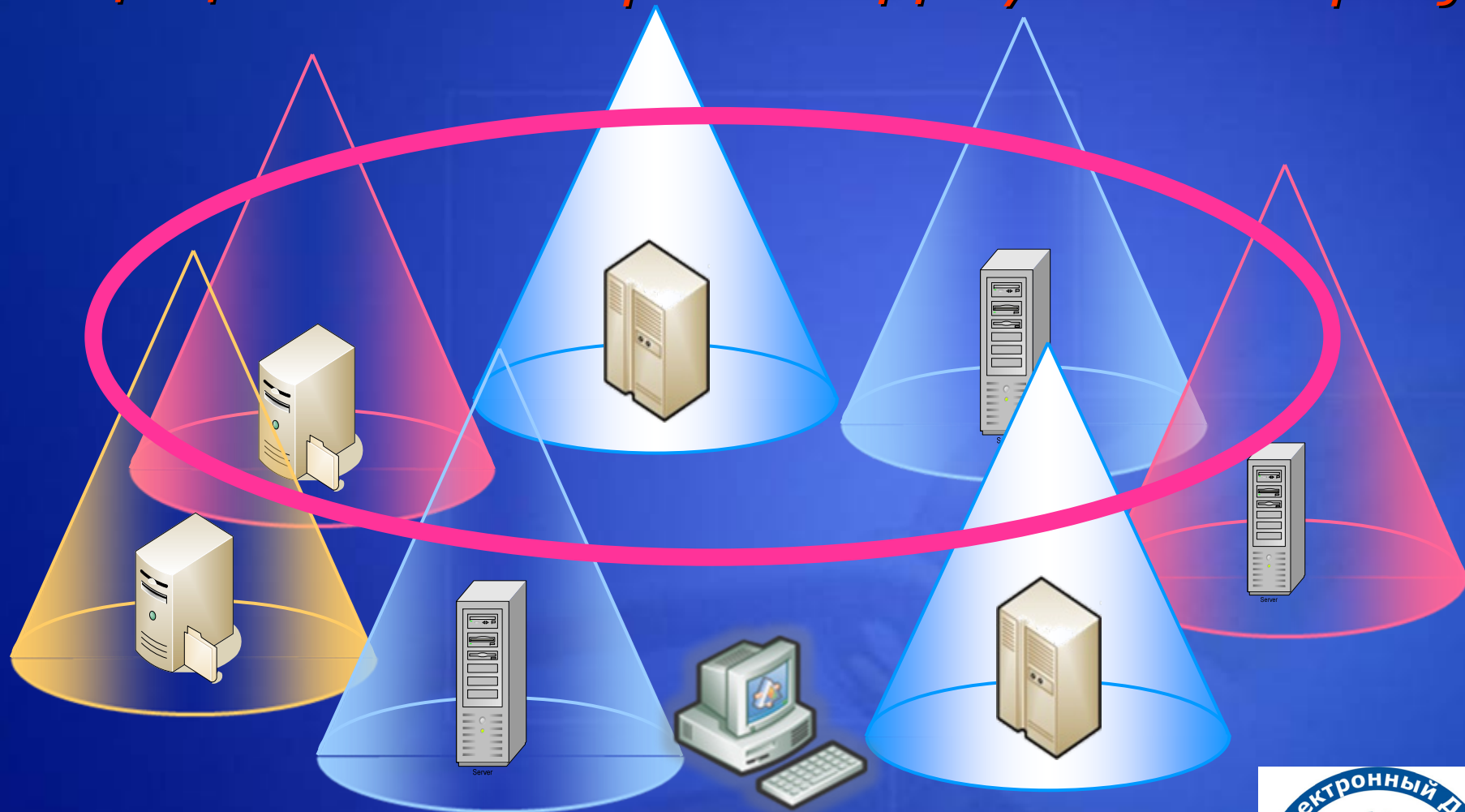
Использование ЭЦП в сфере государственного управления

- ◆ Различные средства защиты информации, в первую очередь криптографические
- ◆ Разрозненные системы защищенного электронного документооборота
- ◆ Отсутствие взаимоувязанных регламентов документооборота (внутриведомственный и межведомственный)



«КриптоСвязь»

{Защищенный Электронный Документооборот}



Научно-производственное предприятие
«ИЖИНФОРМПРОЕКТ»



ЭЛЕКТРОННАЯ
РОССИЯ
ФЕДЕРАЛЬНАЯ ЦЕЛЕВАЯ ПРОГРАММА



«КриптоСвязь»

{Защищенный Электронный Документооборот}

- ◆ «Единый российский криптографический стандарт»
- ◆ Общий регламент защищенного электронного документооборота
- ◆ Общий регламент обеспечения информационной безопасности
- ◆ Межведомственный и внутриведомственный защищенный электронный документооборот
- ◆ Выбор оптимального уровня «включения» («вершины» или «каждый с каждым») в зависимости от структуры документопотоков



Участники системы «КриптоСвязь» {Защищенный Электронный Документооборот}

- ♦ Федеральные органы государственной власти
 - Подразделения Федеральной налоговой службы
 - Подразделения Федеральной службы судебных приставов
- ♦ Органы государственной власти субъекта РФ
 - Министерства и ведомства Удмуртской Республики
 - Комитет по делам ЗАГС УР и органы ЗАГС
- ♦ Органы местного самоуправления
 - Администрации районов Удмуртской Республики
 - Администрация г. Ижевска
 - Муниципальные образования Балезинского района УР
- ♦ Государственные учреждения
 - Удмуртский территориальный фонд ОМС
 - РМИАЦ и лечебно-профилактические учреждения
- ♦ Коммерческие организации



Правовые основы ЗЭД

- ◆ Гражданский кодекс Российской Федерации
- ◆ Федеральные законы Российской Федерации
 - от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»
 - от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
 - от 27.07.2006 № 152-ФЗ «О персональных данных»
 - от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
- ◆ Указы Президента Российской Федерации
 - от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»
 - от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- ◆ Постановления Правительства Российской Федерации
 - от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»
 - от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»



Правовые основы ЗЭД

- ◆ Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005)
- ◆ Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
- ◆ Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 № 149/6/6-622)
- ◆ Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 № 149/54-144)



Использование средств ЭЦП

Федеральный закон РФ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»

- ◆ При создании ключей электронных цифровых подписей должны применяться только **сертифицированные** средства электронной цифровой подписи
- ◆ Использование **несертифицированных** средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления **не допускается**



Государственное регулирование

В соответствии с Постановлением Правительства РФ от 29.12.2007 № 957 средства электронной цифровой подписи относятся к шифровальным (криптографическим) средствам

В соответствии с Федеральным законом от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности»:

- ♦ распространение шифровальных (криптографических) средств
- ♦ техническое обслуживание шифровальных (криптографических) средств
- ♦ предоставление услуг в области шифрования информации подлежат обязательному лицензированию!



Гражданский кодекс РФ (ч.2 ст.160)

Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон



Аналоги собственноручной
подписи



№ 1-ФЗ от 10.01.2002

«Об электронной цифровой подписи»

...электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе...

- + 10 федеральных законов
- + свыше 11 Постановлений Правительства
- + свыше 70 нормативных актов федеральных органов власти



Электронная цифровая подпись
ЭЦП

Юридически значимая ЭЦП и Юридически значимый электронный документ

- ♦ **Юридически значимая ЭЦП:** ЭЦП признается в качестве реквизита электронного документа и лицо её сформировавшее или проверяющее при исполнении документа, несет правовые последствия за это действие
- ♦ **Юридически значимый электронный документ:** ЭД может быть использован в качестве письменного доказательства, как содержащий сведения о фактах, на основании которых устанавливается наличие или отсутствие значимых для дела обстоятельств

Юридически значимая ЭЦП и Юридически значимый электронный документ



Юридически значимая ЭЦП является необходимым, но **недостаточным** условием обеспечения юридической значимости электронного документа

Условия признания равнозначности ЭЦП и собственноручной подписи (ст. 4)

- ◆ сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания
- ◆ подтверждена подлинность электронной цифровой подписи в электронном документе
- ◆ электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи
- ◆ Формирование ключа владельца сертификата с использованием средств ЭЦП
- ◆ Изготовление сертификата ключа подписи с использованием удостоверяющего центра
- ◆ Регистрация УЦ в Едином государственном реестре СКП УЛ УЦ
- ◆ Указание сведений о применении ЭЦП при изготовлении сертификата
- ◆ Формирование ЭЦП электронного документа с проверкой срока действия сертификата и цели применения ЭЦП
- ◆ Верификация ЭЦП электронного документа с проверкой срока действия сертификата и цели применения ЭЦП
- ◆ Проверка действительности и принадлежности сертификата владельцу (доверие УЦ, статус сертификата)

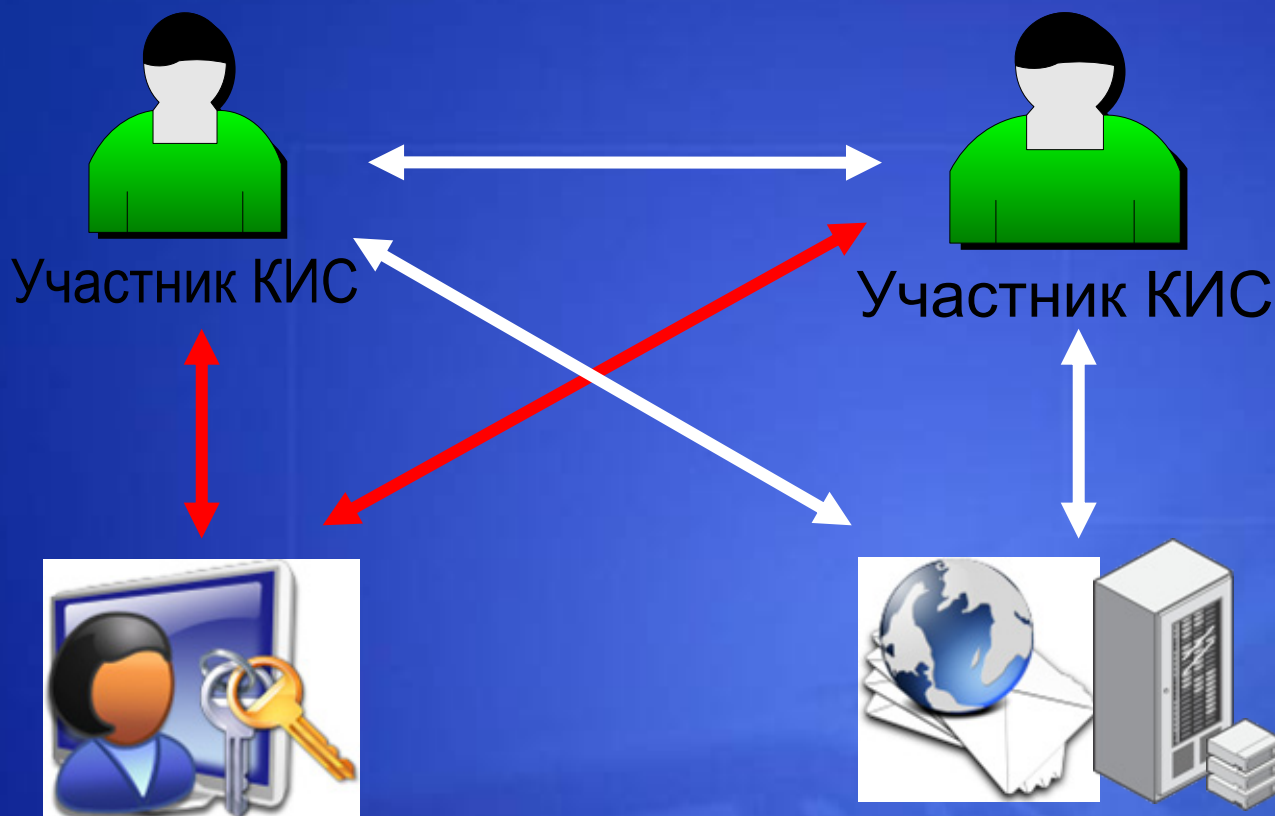


Информационные системы с ЭЦП

- ♦ информационная система **общего пользования** - ИС, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано
- ♦ **корпоративная** информационная система - ИС, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников
 - должна соответствовать требованиям, установленным для ИС общего пользования
 - порядок использования ЭЦП устанавливается решением владельца или соглашением участников
 - регламентация работы системы – по решению владельца или соглашением участников



Система гражданско-правовых отношений КИС



- ◆ Соглашение об использовании ЭЦП в ЭД
- ◆ Соглашение об услугах УЦ

Оператор КИС и УЦ КИС

- ◆ Оператор (организатор) КИС - субъект права, являющийся носителем субъективных прав и юридических обязанностей в части исполнения следующих функций:
 - эксплуатация информационной системы
 - ведение информационных ресурсов и обработка информации в них
 - обеспечение доступа и предоставления информации
 - установление правил использования КИС и информации
- ◆ Удостоверяющий центр КИС - субъект права, являющийся носителем субъективных прав и юридических обязанностей в части:
 - Регистрация владельцев сертификатов ключей подписи
 - Генерация ключей и изготовление сертификатов ключей подписи
 - Предоставление информации о статусе сертификатов, аннулирование, приостановление и возобновление действия сертификатов ключей подписи
 - Подтверждение подлинности ЭЦП в ЭД и сертификатах
- ◆ УЦ может быть структурное подразделение Организатора системы или внешняя организация (аутсорсинг)



Типичные ошибки в постановке цели защищенного взаимодействия

◆ Расплывчатость цели

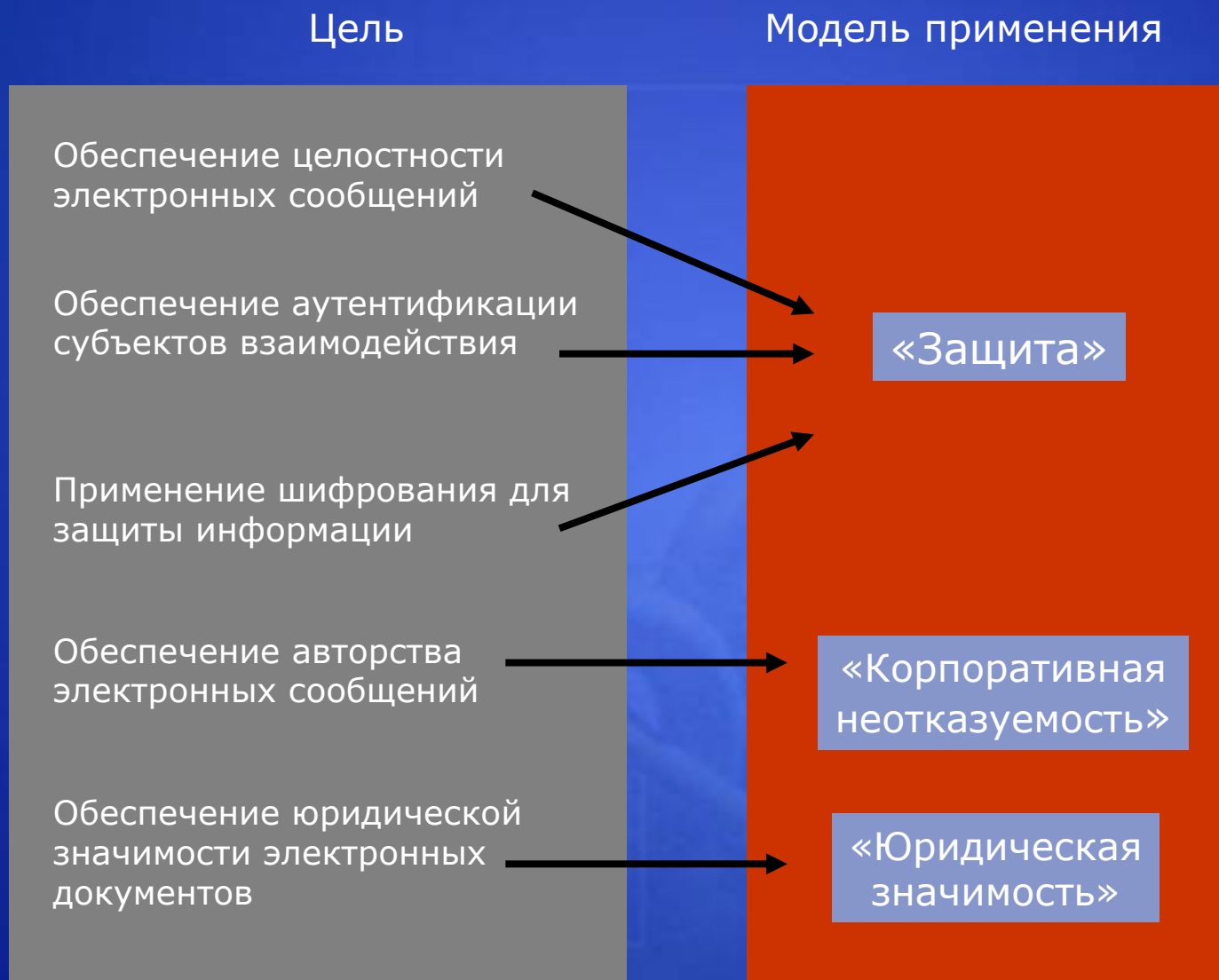
- Нужно защитить информацию с помощью ЭЦП
- Нужен защищенный электронный документооборот

◆ Отсутствие системности

- Необходимо встроить ЭЦП для юридической значимости
- Нужна юридическая значимость ЭЦП
- Нужен удостоверяющий центр для юридической значимости ЭЦП/документов



Типичные ошибки в постановке цели



Ключевые отличия моделей применения

◆ «Защита» vs «Корпоративная неотказуемость»

- «Защита»
 - ◆ нет документов, есть сообщения
- «Корпоративная неотказуемость»
 - ◆ наличие организационных регламентов применения цифровой подписи

◆ «Корпоративная неотказуемость» vs «Юридическая значимость»

- «Корпоративная неотказуемость»
 - ◆ технические и организационные решения определяются владельцем системы
- «Юридическая значимость»
 - ◆ требования к корректности встраивания средств ЭЦП и ее применения
 - ◆ требуется организация удостоверяющего центра как субъекта правоотношений
 - ◆ «внешние» требования к организационным регламентам применения ЭЦП



«Легенды ЭЦП»

- ♦ **Закон «Об ЭЦП» не работает, поэтому ЭЦП применять нельзя** – наличие уголовной, арбитражной и гражданской практики свидетельствует о том, что ФЗ «Об ЭЦП» работает и ЭЦП применима для обеспечения юридической значимости ЭД
- ♦ **Для юридической значимости ЭЦП необходим Федеральный головной удостоверяющий центр** – такой нормы в действующем законодательстве РФ не существует и подобного УЦ не будет ориентировочно до 2010 года
- ♦ **Достаточно использовать сертифицированные средства ЭЦП и юридическая значимость ЭЦП будет обеспечена** – разобрали
- ♦ **Для создания удостоверяющего центра достаточно поставить сервер с программным обеспечением, умеющим изготавливать сертификаты** – разобрали
- ♦ **Если УЦ «кросс-сертифицируются», то будет создано единое пространство легитимности ЭЦП** – обязательство не создает обязанностей для лиц, не участвующих в нем в качестве сторон (для третьих лиц): ч. 2 ст. 308 ГК РФ



«КриптоСвязь»

{Virtual Private Network}

- ◆ Комплексная защита информации при взаимодействии /передаче конфиденциальной информации через открытые каналы передачи данных (Интернет)
 - Безопасность подключения к Интернет,
 - Безопасность распределенной корпоративной сети,
 - Безопасность удаленного доступа в корпоративную сеть
- ◆ Межсетевое экранирование и построение виртуальных частных сетей/VPN (криптографическая аутентификация участников обмена и шифрование трафика)
- ◆ Защита всех прикладных online-сервисов
- ◆ Сертифицированные средства защиты информации



«КриптоСвязь»

{Virtual Private Network}

- ◆ Подключение сетевых объектов: регистрация, инициализация и конфигурация сетевых объектов, изготовление ключей;
- ◆ Абонентское обслуживание: управление средствами защиты информации и техническая поддержка;
- ◆ Работы по техническому сопровождению: монтаж, установка, настройка и сопровождение средств защиты информации и параметров защищенного межсетевого взаимодействия автоматизированного рабочего места защищенного межсетевого взаимодействия (АРМ-VPN)



Почему НПП «Ижинформпроект»?



Спасибо за внимание!

Вопросы?

*Дополнительная информация
www.infotrust.ru security@infotrust.ru
+7 (3412) 918-100
г. Ижевск, ул. Бородина, 21, офис 207*



*Майшев Вадим Владимирович
Заместитель генерального директора по безопасности
mvv@infotrust.ru*



Научно-производственное предприятие
"ИЖИНФОРМПРОЕКТ"